A NEW DATA TRANSFER DATAMATRIX METHODOLGY FOR IP PROTECTION SCHEME

B.Saranya[1] (saranyabullbullya2@gmail.com) PG Scholar,Gnanamani College of Technology.
Mr.R.Poomurugan M.E.,(poomurugan.feb@gmail.com)Assistant Professor,Gnanamani College of Technology.

ABSTRACT

Since digital images are very susceptible to manipulations and alterations, a variety of security problems are introduced. For example, a security centre may wish to authenticate the data received from sensors spread across a facility it is supposed to protect. Another common application is resolving ownership disputes when copyrighted material is distributed illegally. Those problems and needs can be treated by embedding a secret, invisible watermark (WM) in images. A WM is an additional, identifying message, covered under the more significant image raw data, without perceptually changing it. By adding a transparent WM to the image, it can be made possible to detect alterations inflicted upon the image, such as cropping, scaling, covering, blurring and many more. The WM can be added on either a software platform or a hardware platform, each having some benefits and some drawbacks. Although WM implementation on a hardware platform suffers from limited processing power, compared to the software implementation, it features real time capabilities and compact implementations. The advantages of hardware WM implementations are especially enhanced in CMOS imagers, where it is possible to integrate the WM embedded monolithically with the sensor array on the same die

I. Introduction

The advances in very large scale integration (VLSI) semiconductor technology and the system-on-a-chip design paradigm, coupled with the shrinking time-to-market window, have changed the traditional system design methodology. Design reuse and intellectual property (IP), also called virtual component, based designs have become more and more important. IP trading plays a central role in the design-for-reuse methodology and the potential of infringement is growing fast. However, the global awareness of IP protection remains low. The goals of IP protection are to enable IP providers to protect their IPs against unauthorized use and to detect and to trace the use of IPs. According to the IP protection white paper released recently by VSIA, there are three approaches to the problem of securing an IP: deterrent approaches like patents, copyrights, and trade secrets; protection via licensing agreements or encryption; detection mechanisms such as physical tagging, digital watermarking, and finger printing . Of the early efforts on IP protection, only detection mechanisms enable designers to do the so-called self-protection. Other approaches require either time, or money, or both. Using the etection methods, designers embed digital signatures or other traceable marks into IPs a new watermarking technique to solve the copy detection problem. The core concept is to divide the watermark into two parts: the public part which is made visible to the public, and the private part which is only visible for authorized people. Both the public and private watermark are in the form of additional design constraints. Their difference is that the public watermark is embedded in designated locations with known methods to guarantee public detectability, while the private part is embedded in a secret way as in the traditional constraint-based watermark.We use cryptographic techniques for data integrity to deter any attempt of removing or modifying the public watermark. The separation of public watermark and private watermark.

II. Literature Review

As current computer-aided design (CAD) tool and very large scale integration technology capabilities create a new market of reusable digital designs, the economic viability of this new core-based design paradigm is pending on the development of techniques for intellectual property protection. This work presents the first technique that leverages the unique characteristics of field programmable gate arrays (FPGAs) to protect commercial investment in intellectual property through fingerprinting. A hidden encrypted mark is embedded into the physical layout of a digital circuit when it is placed and routed onto the FPGA. This mark uniquely identifies both the circuit origin and original circuit recipient, yet is difficult to detect and/or remove, even via recipient collusion. While this approach imposes additional constraints on the backend CAD tools for circuit place and route, experiments indicate that the performance and area impacts are minimal.

III.Existing System

To prevent the leakage of sensitive information, Existing work to enhance the robustness of watermarking using a large number of small watermarks instead of one large watermark. However, this method will leak a part of the set of watermarking positions after public verification. When infringement occurs repeatedly, more and more watermarking positions will be given away, which facilitates the attacker to remove more watermarks. Existing a publicly detectable VLSIwatermarking technique that embeds an independent public watermark for public verification. However, this method is not suitable for FPGA designs because public watermarking positions will be leaked after public verification, hence attackers can tamper, remove, or cover the public watermark in the bitstream of FPGA design,

which would result in the wrong verification of IP.The purpose of public verification is to reduce or eliminate the dependence of one party on the reliability of the other parties,reduce the constraint of the verifier in protocol, and improve the security of the entire scheme. When a dispute occurs among the parties involved in the protocol, public verification is convenient for the arbitration of dispute.

IV.Proposed System

In this paper, a new publicly verifiable watermarking detection scheme based on chaotic sequences is proposed to address the issues that the FPGA watermarking technique may leak the sensitive information and the existing zero knowledge FPGA watermarking detection scheme is vulnerable to embedding attacks. This scheme comprises the following.

1) The watermark is hidden in the unused lookup table (LUT) of used Slice, and the watermarking content of LUT of ˆ I is encrypted to prevent the leakage of watermarking content.

2) Since chaotic sequences have high randomness and low cross correlation, we can generate a real number chaotic sequence in each round of verification. The chaotic sequence is binarized into ρ, which is used as an input to the position mapping algorithm $\pi(\rho)$ to control the location permutation of LUTs in FPGA bitstream, i.e., $\pi(\rho)$ is applied to ˆ I to get the scrambled design ξ. Then ρ and the position of the watermark in ξ are used to interact between the prover and verifier. With the zeroknowledge protocol, the prover makes the verifier believe the watermark existing in IP without leaking the position information.

3) Timestamp is introduced to resist embedding attack to prevent dishonest IP buyers from denying.

A new watermarking technique taking advantage of Data Matrix as well as encryption keys. The Data Matrix not only recovers the original data by an error checking and correction algorithm, even when its high-density data storage and barcode are damaged, but also encrypts the copyright verification information by randomization of the barcode, including ownership keys. Furthermore, the encryption keys and the patterns are used to localize the watermark, and make the watermark robust against attacks, respectively. Through the comparison experiments of the copyright information extracted from the watermark, we can verify that the proposed method has good quality and is robust to various attacks, such as JPEG compression.

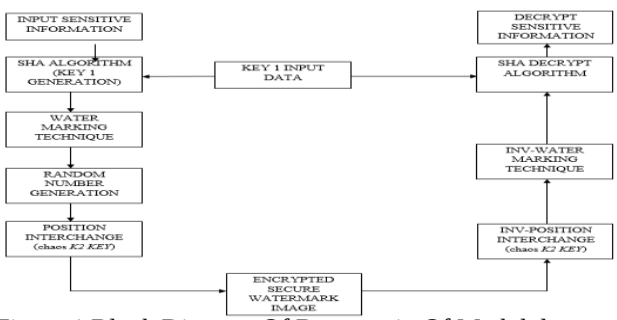

Figure 1 Block Diagram Of Datamatrix Of Methdology

IV Result

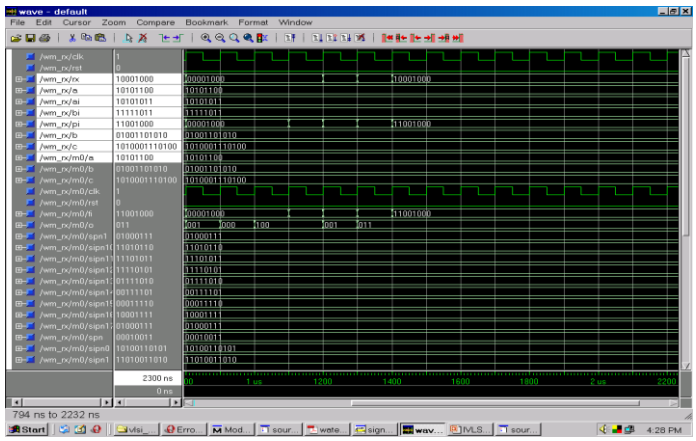

Figure 2 Simulation result for Datamatrix Of Methdology

IV. Conclusion

Our work is motivated by the proliferation of IP reuse in VLSI design and the potential of it being illegally redistributed and misused. We propose a public–private watermarking method, the first that allows the IP's authorship to be established easily and publicly. We achieve this by allowing part of the watermark to be public. We use cryptographic techniques, in particular techniques for data integrity, to protect the public watermark from forgery. Using the traditional constraint-based watermark as private part, this public–private watermarking scheme is capable of providing public detectability with no degradation on the watermark's strength.We explain the basic approach and develop specific techniques for various classes of VLSI CAD problems. The newapproach is compatible with all the existing watermarking techniques. With the help from organizations pushing for design standards, for example VSIA, this method has the potential of solving eventually the IP protection problem.

REFERENCES

[1] A. Adelsbach, B. Pfitzmann, and A. Sadeghi, "Proving ownership of digital content," in *Proc. 3rd Int Information Hiding Workshop*, Sept 1999, pp. 126–141.

[2] A. E. Caldwell, H. Choi, A. B. Kahng, S. Mantik, M. Potkonjak, G. Qu, and J. L.Wong, "Effective iterative techniques for fingerprinting design IP," *36th ACM/IEEE Design Automation Conf. Proc.*, pp. 843–848, June 1999.

[3] E. Charbon, "Hierarchical watermarking in IC design," in *Proc. IEEE 1998 Custom Integrated Circuits Conf.*, May 1998, pp. 295–298.

[4] E. Charbon and I. Torunoglu, "Copyright protection of designs based on multi source IP's," in *Proc. IEEE/ACM Int. Conf. Computer-Aided*

Design, Nov. 1999, pp. 591–595. [5] S. Craver, "Zero knowledge watermark detection," in *Proc. 3rd Int. Information Hiding Workshop*, Sept. 1999, pp. 102–115.

[6] F. Hartung and B. Girod, "Fast public-key watermarking of compressed video," in *Proc. IEEE Int. Conf. Image Processing*, Oct. 1997, pp. 528–531.

[7] I. Hong and M. Potkonjak, "Behavioral synthesis techniques for intellectual property protection," *Proc. 36th ACM/IEEE Design Automation Conf. Proc.*, pp. 849–854, June 1999.
[8] A. B. Kahng, J. Lach, W. H. Mangione-Smith, S. Mantik, I. L. Markov, M. Potkonjak, P. Tucker, H. Wang, and G. Wolfe, "Watermarking techniques for intellectual property protection," *35th ACM/IEEE Design Automation Conf. Proc.*, pp. 776–781, June 1998.
[9] A. B. Kahng, D. Kirovski, S. Mantik, M. Potkonjak, and J. L. Wong, "Copy detection for intellectual property protection of VLSI design," in *Proc. IEEE/ACM Int. Conf. Computer-Aided Design*, Nov. 1999, pp. 600–604.
[10] D. Kirovski, Y. Hwang, M. Potkonjak, and J. Cong, "Intellectual property protection by watermarking combinational logic synthesis
solutions," in *Proc. IEEE/ACM Int. Conf. Computer-Aided Design*, Nov. 1998, pp. 194–198.
[11] D. Kirovski, D. Liu, J. L. Wong, and M. Potkonjak, "Forensic engineering techniques for VLSI CAD tools," *37th ACM/IEEE Design Automation Conf. Proc.*, pp. 581–586, June 2000.
[12] J. Lach, W. H. Mangione-Smith, and M. Potkonjak, "FPGA fingerprinting techniques for protecting intellectual property," *Proc. IEEE
1998 Custom Integrated Circuits Conf.*, pp. 299–302, May 1998.
[13] , "Signature hiding techniques for FPGA intellectual property protection," in *Proc. IEEE/ACM Int. Conf. Computer-Aided Design*, Nov.
1998, pp. 186–189.
[14] A. L. Oliveira, "Robust techniques for watermarking sequential circuit designs," *36th ACM/IEEE Design Automation Conf. Proc.*, pp. 837–842, June 1999.
[15] B. Pfitzmann, "Information hiding terminology," in *1st Int. Information Hiding Workshop*, May 1996, pp. 347–350.
[16] G. Qu, "Publicly detectable watermarking for intellectual property authentication in vlsi design," Univ. Maryland Inst. Advanced Computer Studies (UMIACS), UMIACS-TR-2002-17, 2002.
[17] G. Qu and M. Potkonjak, "Analysis of watermarking techniques for graph coloring problem," in *Proc. IEEE/ACM Int. Conf. Computer-
Aided Design*, Nov. 1998, pp. 190–193.
[18] G. Qu, J. L. Wong, and M. Potkonjak, "Optimization-intensive watermarking techniques for decision problems," *36th ACM/IEEE Design Automation Conf. Proc.*, pp. 33–36, June 1999.
[19] R. L. Rivest. (1992) The MD5 Message-Digest Algorithm. [Online]. Available: http:// www.cis.ohio-state.edu/htbin/rfc/rfc1321.html
[20] N. A. Sherwani, *Algorithms for VLSI Physical Design Automation*, 3rd ed. New York: Kluwer, 1999.